Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) In a wireless data communications system wherein mobile units communicate with a computer using access points, and wherein said system operates according to a protocol specifying a format for data message packets and said data message packets contain state information for said mobile units, a method for detecting unauthorized access attempts to the system, comprising:

forwarding one or more data packets received by said access points to a computer; and

maintaining a state table on said computer, said state table storing state information for said mobile units; and

operating said computer to compare format and state information of said one or more received data packets to selected requirements of said protocol-specified format and said stored state information, and signaling an alert if said packets deviate from said protocol-specified format or said stored state information.

2. (original) A method as specified in claim 1 wherein said protocol-specified format includes a header message portion and wherein said comparing of format comprises comparing format of said header message portion to said protocol-specified format.

3. (currently amended) A method as specified in claim 2 wherein said protocol is one of IEEE Standards 802.11a/b/g.

4. (currently amended) A method as specified in claim 2 wherein said protocol is one of IEEE Standards 802.11a/b/g having a frame control field in said header message portion and wherein said comparing of format comprises comparing format of said frame control field.

5. (currently amended) A method as specified in claim 1 wherein said protocol is one of IEEE Standards 802.11a/b/g, and further wherein said one or more received data packets comprise IEEE Standard 802.11a/b/g Management Frames.

6. (currently amended) A method as specified in claim 1 wherein said protocol is one of IEEE Standards 802.11a/b/g, and further wherein said one or more received data packets comprise IEEE Standard 802.11a/b/g Control Frames.

7. (currently amended) A method as specified in claim 1 wherein said protocol is one of IEEE Standards 802.11a/b/g, and further wherein said one or more received data packets comprise a first WEP flag.

8. (currently amended) A method as specified in claim 7 wherein said packets have a first WEP flag value which is inconsistent with a second WEP value stored in [[a]] said state table on said computer.

9. (currently amended) A method as specified in claim 1 wherein said one or more received data packets comprise a first Protocol Version value which is inconsistent with a second Protocol Version value stored in [[a]] said state table on said computer.

10. (original) A method as specified in claim 1 wherein said one or more received data packets comprise a source MAC address which is a multicast address.

11. (original) A method as specified in claim 1 wherein said one or more received data packets comprise a source MAC address which is a broadcast address.

12. (currently amended) A method as specified in claim 3 wherein said one or more received data packets comprise a first Power Management state variable which is inconsistent with a second Power Management state variable value stored in [[a]] said state table on said computer.

13. (currently amended) A method as specified in claim 3 wherein the step of operating said computer further comprises checking a More Data field of said received data packets for a value of "1" and further monitoring said access points for a possible denial of service attack.

14. (original) A method as specified in claim 3 wherein said one or more received data packets comprise an unsupported Type value.

15. (original) A method as specified in claim 3 wherein said one or more received data packets comprise an unsupported SubType value.

16. (original) A method as specified in claim 1 wherein said one or more received data packets comprise a spoofed MAC address.

17. (original) A method as specified in claim 3 wherein said one or more received data packets comprise a frame of length which is inconsistent with said protocol-specified format.

18. (canceled)

19. (currently amended) In a wireless data communications system wherein mobile units communicate with a computer using access points, and wherein said system operates according to a protocol specifying a format for data message packets and said data message packets contain state information for said access points, a method for detecting unauthorized access attempts to the system, comprising:

forwarding one or more data packets received by said mobile units to a computer; and

maintaining a state table on said computer, said state table storing state information for said access points; and

operating said computer to compare format and state information of said one or more received data packets to selected requirements of said protocol-specified format and said stored state information, and signaling an alert if said packets deviate from said protocol-specified format or said stored state information.

20. (original) A method as specified in claim 19 wherein said protocol-specified format includes a header message portion and wherein said comparing of format comprises comparing format of said header message portion to said protocol-specified format.

21. (currently amended) A method as specified in claim 20 wherein said protocol is one of IEEE Standards 802.11a/b/g having a frame control field in said header message portion and wherein said comparing of format comprises comparing format of said frame control field.

22. (currently amended) A method as specified in claim 19 wherein said protocol is one of IEEE Standards 802.11a/b/g, and further wherein said one or more received data packets comprise IEEE Standard 802.11a/b/g Management Frames.

23. (currently amended) A method as specified in claim ~~18~~ 19 wherein said protocol is one of IEEE Standards 802.11a/b/g, and further wherein said one or more received data packets comprise IEEE Standard 802.11a/b/g Control Frames.

24. (currently amended) A method as specified in claim 19 wherein said protocol is one of IEEE Standards 802.11a/b/g.

25. (currently amended) A method as specified in claim 19 wherein said protocol is one of IEEE Standards 802.11a/b/g, and further wherein said one or more received data packets comprise a first WEP flag.

26. (currently amended) A method as specified in claim 25 wherein said packets have a first WEP flag value which is inconsistent with a second WEP value stored in [[a]] said state table on said computer.

27. (currently amended) A method as specified in claim 25 wherein said one or more received data packets comprise a first Protocol Version value which is inconsistent with a second Protocol Version value stored in [[a]] said state table on said computer.

28. (original) A method as specified in claim 24 wherein said one or more received data packets comprise a source MAC address which is a multicast address.

29. (original) A method as specified in claim 24 wherein said one or more received data packets comprise a source MAC address which is a broadcast address.

30. (currently amended) A method as specified in claim 24 wherein said one or more received data packets comprise a first Power Management state variable which is inconsistent with a second Power Management state variable value stored in [[a]] said state table on said computer.

31. (currently amended) A method as specified in claim 24 wherein the step of operating said computer further comprises checking a More Data field of said received data packets for a value of "1" and further monitoring said access points for a possible denial of service attack.

32. (original) A method as specified in claim 24 wherein said one or more received data packets comprise an unsupported Type value.

33. (original) A method as specified in claim 24 wherein said one or more received data packets comprise an unsupported SubType value.

34. (original) A method as specified in claim 24 wherein said one or more received data packets comprise a spoofed MAC address.

35. (original) A method as specified in claim 24 wherein said one or more received data packets comprise a frame of length which is inconsistent with said protocol-specified format.

36-39. (canceled)